REMARKS

The Examiner has objected to Claims 1, 17, and 34 as not being clear as to which macro is applied. Specifically, the Examiner objected to "the sets of indices and macro virus definition data files ...organized into a hierarchy ...to which the macro applies." Applicant respectfully asserts that it is sufficient clear, from the claim language alone, that "the sets of the indices and the macro virus definition data files [are]... organized into a hierarchy according to macro virus families based on a type of application to which the macro applies" (emphasis added), as claimed by applicant. This claim language is supported in the specification on page 8, lines 10-11. Specifically, the specification discloses that "[t]he macro virus definitions database 28 is hierarchically organized into macro virus families based on the type of application to which the macro applies" (emphasis added). Thus, it is clear that the macro is applies "to a type of application."

Additionally, the Examiner has objected to Claims 1, 17, and 34 as failing to have support in the specification. Specifically, the Examiner argued that 'the phrase "the sets of the indices and the macro virus definition data files being organized into a hierarchy" does not appear to be consistent with the specification referring to a database being organized into a hierarchy and not the sets of indices and macro virus definition data files; the sets of indices and macro virus definition data files are just part of the database.' However, the specification states "[b]y way of example, the macro virus definitions database 28 can include a root directory 29, below which word processor 30, spreadsheet 31, presentation 32, and generic 33 subdirectories can contain individual indices and macro virus definition data (*.dat*) files, as further described below with reference to FIGURE 4" (emphasis added – see page 8, lines 12-16). Additionally, the specification discloses that "[a]n index maintained in index files, *route.idx* 41 stores pointers to locations in individual *.dat* files *000000001.dat* 42, *000000002.dat* 43 and *000000002.dat* 44 files" (emphasis added) and "[e]ach of the *.dat* files 42-44 store information describing a macro virus family, as characterized by the replication method used by the virus" (emphasis added – see page 8, lines 20-24). See also Figure 4. Thus, the specification clearly supports the claimed technique where "the sets of the indices and the

macro virus definition data files being organized into a hierarchy," as claimed by applicant.

The Examiner has rejected Claims 1-5, 12-13, 15, 17-21, 28-29, 31, 33-35, 38-40, and 43-44 under 35 U.S.C. 103(a) as being unpatentable over Chen (U.S. Patent No. 5,951,698) in view of Bates et al. (U.S. Patent No. 6,721,721) in view of Perelson et al. (U.S. Patent No. 5,448,668). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to the independent claims. Specifically, applicant has amended the independent claims to at least substantially include the subject matter of former dependent Claims 2-5 et al.

With respect to the independent claims, the Examiner, in blanket manner, has relied on columns 5-6, column 8, line 20 through column 9, line 15, and column 12 in Chen to make a prior art showing of applicant's claimed technique "the sets of the indices and the macro virus definition data files being organized into a hierarchy according to macro virus families based on a type of application to which the macro applies" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpts from columns 5-6 in Chen relied upon by the Examiner only disclose that "a virus information module 308 provides comparison data for the detection of viruses in macros and the treatment of macros with viruses, and the data buffer 312 provides for the storage of information which is used in the detection and correction of macro viruses" (emphasis added). However, simply disclosing "a virus information module 308 provides comparison data for the detection of viruses in macros and the treatment of macros with viruses" clearly fails to meet a technique where "the sets of the indices and the macro virus definition data files being organized into a hierarchy" (emphasis added), as claimed.

In addition, applicant respectfully asserts that the excerpts from columns 8, line 20 through column 9, line 15 merely suggest that "[t]he comparison data includes sets of instruction identifiers which are used to identify combinations of suspect instructions in

the decoded macro" (emphasis added) where "[a]n exemplary set of instruction identifiers includes first and second suspect instruction identifiers" (emphasis added). However, the disclosure that "[t]he comparison data includes sets of instruction identifiers" simply fails to meet a technique where "the sets of the indices and the macro virus definition data files being organized into a hierarchy" (emphasis added), as claimed by applicant.

Further, applicant respectfully asserts that the excerpts from column 12 in Chen relied upon by the Examiner disclose that "[i]f the file format indicates a template file is included, then the targeted file may include an embedded macro" (emphasis added). However, disclosing that a template file may include an embedded macro clearly fails to even suggest a technique where "the sets of the indices and the macro virus definition data files being organized into a hierarchy according to macro virus families based on a type of application to which the macro applies" (emphasis added), as claimed by applicant.

In the Office Action mailed 03/15/2006, the Examiner argued that "Bates discloses a virus database with indices and data files being organized into a hierarchy, as disclosed by Bates it is well known that a database may be an index and/or directory based database (see column 6, lines 35 through column 8, line 15, with emphasis on column 8, lines 4-15 and column 11, lines 1-11) which implicitly has a hierarchical structure as data files are arranged in a well-organized manner." Applicant respectfully asserts that the excerpts from Bates simply teach that "[i]n the case of an index-based or directory-based search engine, typically a result set includes identifiers of a plurality of index or directory records in the respective database, with each such record identifying one or more files, e.g., via URL's stored in such records" (emphasis added). Clearly, the "index-based or directory-based search engine" (emphasis added) with the result set containing "index or directory records" (emphasis added) simply fails to even suggest "the sets of the indices and the macro virus definition data files being organized into a hierarchy according to macro virus families based on a type of application to which the macro applies" (emphasis added), as claimed by applicant.

In addition, in the Office Action mailed 03/15/2006, the Examiner argued that "Chen discloses a data table including sets of instruction identifier stored in the virus information module (column 14, line 65 through column 15)." Applicant respectfully asserts that the excerpts from Chen merely disclose that "[t]he exemplary data table 900 includes rows 902 which correspond to several different sets of instruction identifiers." However, merely disclosing that "rows ... correspond to several different sets of instruction identifiers" fails to even suggest "the sets of the indices and the macro virus definition data files being organized into a hierarchy according to macro virus families based on a type of application to which the macro applies" (emphasis added), as claimed by applicant.

Further, with respect to the independent claims, the Examiner has relied on column 15, lines 1-12 in Chen to make a prior art showing of applicant's claimed technique "wherein a parameter is utilized for specifying a threshold to matches of commonly shared at least one of string constants and source code text" (see this or similar, but not necessarily identical language in the independent claims).

> "...table 900 includes rows 902 which correspond to several different sets of instruction identifiers. Columns identifying the sets of instruction identifiers 903, their instruction identifier numbers 904 and text and corresponding hexadecimal representations 905 of the binary code for the instruction identifiers are included. Preferably, two instruction identifiers are included in each set of instruction identifiers, but additional instruction identifiers can be included in a set. **Additionally, a positive macro virus determination can be made based upon detection of two out of three instruction identifiers or some other subset of identifiers.** The data table 900 is exemplary only. The comparison data may be variously stored in the virus information module 308." (Chen, Col. 15, lines 1-15 - emphasis added)

Applicant respectfully asserts that the excerpt from Chen relied upon by the Examiner merely suggests that "a positive macro virus determination can be made based upon detection of two out of three instruction identifiers or some other subset of identifiers" (emphasis added). However, the excerpt from Chen simply fails to even

suggest a technique "wherein a parameter is utilized for specifying a threshold to matches of commonly shared at least one of string constants and source code text" (emphasis added), as claimed by applicant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has incorporated the subject matter of former Claims 2-5 et al. into the independent claims, as follows:

> "wherein the macro virus definition data files are indexed into the macro virus families categorized by a replication method employed;
>
> wherein the suspect string comprises part of the suspect file, the suspect file comprising a plurality of individual suspect strings;
>
> wherein the macro virus checker identifies the replication method common to the plurality of the individual suspect strings in the suspect file;
>
> wherein the macro virus checker identifies the macro virus family by which the common replication method is indexed" (see this or similar, but not necessarily identical language in the independent claims).

With respect to the subject matter of former Claim 2 et al. (now at least substantially incorporated into the independent claims), the Examiner has relied on Column 8 in the Chen reference to make a prior art showing of applicant's claimed technique where "the macro virus definition data files being indexed into the macro virus families categorized by a replication method employed" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpt from Chen relied upon by the Examiner teaches that "[t]he comparison data includes sets of instruction identifiers which are used to identify combinations of suspect instructions in the decoded macro" (emphasis added). Chen continues to teach that "[a]n exemplary set of instruction identifiers includes first and second suspect instruction identifiers" (emphasis added). However, disclosing a set of instruction identifiers which includes first and second suspect instruction identifiers simply fails to meet a technique where "the macro virus definition data files [are] indexed into the macro virus families categorized by a replication method employed" (emphasis added), as claimed by applicant.

With respect to the subject matter of former Claims 3-4 et al. (now at least substantially incorporated into the independent claims), the Examiner has relied on the following excerpt from the Chen reference to make a prior art showing of applicant's claimed technique "wherein the suspect string comprises part of the suspect file comprising a plurality of individual suspect strings" and "the macro virus checker identifying a replication method common to a plurality of the individual suspect strings in the suspect file" (see this or similar, but not necessarily identical language in the independent claims).

> "A macro virus reproduction instruction is a type that allows replication of the macro virus. For example, the MacroCopy instruction copies a macro, and, if the macro is infected, all of its harmful instructions, from a source to a destination. Other instructions, such as Organizer .copy, also facilitate macro virus reproduction. It is understood that various alternative instructions can facilitate macro virus reproduction." (Chen, Col. 14, lines 16 et seq. - emphasis added)

Applicant respectfully asserts that the excerpt from Chen relied upon by the Examiner merely teaches that "[a] macro virus reproduction instruction is a type that allows replication of the macro virus." Chen discloses that "the MacroCopy instruction copies a macro" and "Organizer .copy, also facilitate[s] macro virus reproduction." However, simply disclosing macro virus reproduction instructions clearly fails to meet a technique where "the macro virus checker identifying a replication method common to a plurality of the individual suspect strings in the suspect file" (emphasis added), as claimed by applicant.

With respect to the subject matter of former Claim 5 et al. (now at least substantially incorporated into the independent claims), the Examiner has relied on column 14, lines 16 et seq., and column 8, line 40 through column 9, line 15 from the Chen reference to make a prior art showing of applicant's claimed " macro virus checker identifying the macro virus family by which the common replication method is indexed" (see this or similar, but not necessarily identical language in the independent claims).

Applicant respectfully asserts that the excerpts from Chen relied upon by the Examiner teach that "[t]he macro virus scanning module 304 includes routines to detect macro instruction combinations which are very likely to be used by macro viruses." Specifically, Chen suggests that "[t]he combination of a macro enablement instruction and a macro reproduction instruction indicates a macro virus since such instructions allow replication and execution of a macro in a destination file, two common characteristics of macro viruses" (emphasis added). Chen continues to teach that "if it is determined that the macro includes the combination of suspect instructions defined and identified by the set of instruction identifiers, then it is determined that the macro is infected by an unknown virus corresponding to that set of data" (emphasis added). However, disclosing that if "the macro includes the combination of suspect instructions defined and identified by the set of instruction identifiers, then it is determined that the macro is infected by an unknown virus" simply fails to even suggest a " macro virus checker identifying the macro virus family by which the common replication method is

indexed" (emphasis added), as claimed by applicant. Further, indicating that "the macro is infected by an unknown virus" (emphasis added) clearly does not even suggest a "macro virus checker identifyi[es] the macro virus family" as claimed by applicant.

Again, applicant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art references, when combined, fail to teach or suggest all of the claim limitations, as noted above. Thus, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P373).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100